Journal of Fundamental and Applied Sciences

ISSN 1112-9867

Available online at http://www.jfas.info

Research Article

Special Issue

STUDYING PRIVACY IN ELECTRONIC VOTING PROTOCOLS AND COMPARING ITS METHODS OF PROVISION

M. Pourmonfared Azimi[1] and M. A. Doostdari[2,*]

[1]Department of Computer Engineering, Laboratory of electronic voting, Shahed University, Tehran, Iran

[2]Assistant Professor, Department of Computer Engineering, Shahed University, Tehran, Iran

Published online: 15 May 2016

ABSTRACT

In the present paper first by introducing the inherent requirements of electronic voting and comparing them with the ones provided by researchers until the present time, a formal definition of privacy in electronic voting was given. Then by taking into consideration the privacy, developments in providing electronic voting protocols were investigated. Then results of the investigations were given and the methods of providing privacy in the protocols were introduced. In the end these methods were examined and compared and the homomorphic encryption was proposed as the best method.

Keywords: electronic voting; privacy; homomorphic encryption; blind signature.

Author Correspondence, e-mail: doostari@shahed.ac.ir

doi: http://dx.doi.org/10.4314/jfas.v8i3s.175

1- INTRODUCTION

The fast growing usage of electronic services and emergence of different internet services in forms of websites or special devices for financial services and banking and also utilizing electronic beds for sensitive military measures and information exchange, has caused the appearance of concepts such as electronic governance in the present time. In the structure of electronic governance, as parallel with services provided in form of electronic government, concepts such as electronic democracy are discussed. In electronic democracy the most prominent index of a structure based on public demand is electronic election. In recent years great efforts have been made around the world for realization of electronic election. Each one of the efforts has been successful relatively. In countries such as Estonia and the U.S electronic election is performed in real scale [1,2].

While designing an electronic voting protocol, one of the most fundamental matters which is the inherent requirement and specification of voting system is protecting votes of voters. This means that no one is able to create a connection between the voter and his/her vote. Moreover accuracy of the counted vote in the final result and its inspection capability is an important issue for the voter. Basically the general direction in designing such a system is to exert real outlook of people in election; for this reason issues such as preventing forcing the voter or buying and selling votes are clearly included in this concept.

Chawem in a paper about hash networks [3] has mentioned one of its functions in electronic voting which led to academic interest in developing such systems. In years after that theoretical voting plans were suggested with diverse approaches. In most of these plans in order to create a sense of trust in the voter, the capability of following the vote is given to the voter; in such a way that while voting the voter received some information through which he/she could follow his/her vote to the end. When the voter can give his/her vote to another entity in the system, problems such as buy and sell of vote or the possibility of forcing the voter are created in election process. Therefore as shown in [4], existence of receipt can be a threat for privacy of vote. Although designers and developers were aware of necessity of the vote privacy but due to theoretical and technical deficiencies were unsuccessful in reaching their goals. All plans provided until that time created a receipt for the voter in voting proves and according to the new outlook [4] were unsuccessful in creating privacy of the vote. Introduction of this new specification and attempt to supply it has led to emergence of a new path in designing voting systems called developing systems without receipt.

Furthermore absence of receipt or impossibility of proving vote even with receipt, could not prevent forcing the voters to vote, therefore [5] proposed the need of absence of force in voting as another segment of privacy concept (upper line in figure 1)

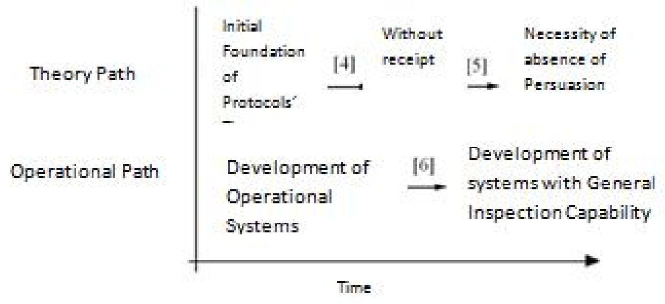
Theory Path
Operational Path
Initial Foundation of Protocols'
[4]
Without receipt
[5]
Necessity of absence of Persuasion
Development of Operational Systems
[6]
Development of systems with General Inspection Capability
Time

Fig.1. Development of Electronic Voting Systems

Being certain of providing the feature of absence of receipt and absence of force caused utilization of complicated and newfangled acts of encryption in plans. This complicated approach deferred the election in electronic form in the real world. Chawem recognized this problem and in [6] provided a voting plan with very simple mechanism in order to inspect the result. This innovation rejuvenated the development of operational systems that combined inspection capability and privacy. Generally these specific types of plans are called systems with general inspection capability (lower line in figure 1).

In this paper we extract inherent requirements of system from initial and obvious definitions of a voting system. Then a classification of requirements which includes all matters proposed by researchers until the present time is suggested. Moreover the relationship of each one of the requirements with inherent requirements of system is determined. By using this overall framework a formal definition of privacy in voting is given.

In the present paper fifteen important and effective theoretical protocols in development process of systems are investigated and according to the introduced overall framework, features of each one of them are enumerated. Blind signature and homomorphic encryption are utilized in most of these protocols. In homomorphic encryption it is possible to obtain the desired answer by only one step of decryption, therefore this method is specially used in this research which is reflected in conclusion section of the paper. In the end according to these investigations the results are presented in tables. These tables give some information regarding level of success of each one of the plans that looking from outlook of privacy is the purpose of this paper and on the other hand is the level of success of inspection capability satisfaction as a mechanism to evaluate operational accuracy of plan. After that according to the observations and findings of research the suitable mechanism in designing protocols to supply privacy is suggested from among the utilized mechanisms.

2- PRIVACY IN ELECTRONIC VOTING

To explain necessities of investigating privacy in voting, first we need to know the inherent specifications of a sample system according to the common definition of a basic electronic voting system. Then by introducing an overall framework of system requirements, the formal definition of privacy in electronic voting is given.

2-1 Inherent Requirements of an Electronic Voting System

The starting point of this analysis is giving attention to the acceptance criterion of electronic election system. Clearly this is the most essential need of a basic voting system. The demand that a voter eventually has from an election system is that the system output be a true consequence of system inputs and its accuracy can be inspected. This concept in fact indicates the acceptance criterion in election. The election is acceptable at the time when it is accepted by people. The voters confirm correctness of voting when this correctness can be verified with some mechanisms. Having this in mind if requirement is shown with R and initial requirement with IR, the two initial requirements of system are introduced in the following way:

IR1: the outcome truly indicates preference of voters’ group

IR2: correctness and accuracy of the outcome can be verified using a method.

In fact the election system collects votes of every individual person and finally specifies the outcome which has been preferred and chosen by group. Therefore the voters must act truthfully from the time of entering system until the end and every person should not be able to vote more than one time. With this definition the requirement of IR1 can be expanded as following:

- R1 All voters must be free in voting
- R2 Only the votes given by voters must be counted in the end
- R3 Every voter can vote only one time
- R4 The outcome of system be truly dependent on all given votes

The requirement R1 refers to the freedom of voters; this means that in voting the voter must feel free of any kind of external interference and feel no restriction in expressing his/her idea. This feature is called “freedom” in voting. Therefore this concept indicates the ultimate level of providing privacy in the system.

It should be noted that all voters do not need to vote and this is not discussed as a specification of voting system. Therefore the matter of being or not being absent in voting is not an inherent requirement of voting system and this is not discussed here.

In requirement R4 the true dependence of outcome to every individual vote is considered; this means that the outcome is dependent on each one of the votes and not to any other thing. Therefore this requirement can be expanded in the following way:

R4a The outcome of counting be resulted from all votes

R4b Every individual vote be counted in the final outcome

R4c The outcome be dependent on nothing else but votes

While investigating initial requirement of IR2 we’ll reach at the concept of “capability of accuracy inspection” but the voters do not know the number of given votes. Of course this does not create a problem; because if everyone knew what vote is counted then we did not need voting system. Therefore the voter must only be able to check if his/her vote is counted accurately and outcome is according to a list of given votes. Therefore IR2 is expanded as following:

- R5 Every voter must be able to check if his/her vote is counted accurately in the final outcome
- R6 Every voter must be able to check if the final outcome is the result of all votes given truly and nothing else.

Table 1. Inherent Requirements of System

Initial Requirement	Inherent Requirement	Requirement Description
IR1	R1	All voters must be free in voting
IR1	R2	Only the votes given by voters must be counted in the end
IR1	R3	Every voter can vote only one time
IR1	R4	The outcome of system be truly

		dependent on all given votes
R4	R4a	The outcome of counting be resulted from all votes
R4	R4b	Every individual vote be counted in the final outcome
R4	R4c	The outcome be dependent on nothing else but votes
IR2	R5	Every voter must be able to check if his/her vote is counted accurately in the final outcome
IR2	R6	Every voter must be able to check if the final outcome is the result of all votes given truly and nothing else

In table 1 the points mentioned above are stated briefly. In the table the initial requirement of every requirement is also specified. For instance as can be seen in the first row of table, R1 requirement is derived from IR1 initial requirement.

2-2 Classification of Electronic Voting Requirements and their Relation with Privacy

When the requirements of a voting system are looked at from outlook of the related literature, we are faced with a collection of various terms and phrases used to explain these requirements. This diversity creates a nature that lacks generalization of some of the terms coined recently. Sentences discovered newly are changed to a new requirement creating new term. Some of the more general requirements are accompanied with a new term covering previous and major requirements. Furthermore the concepts are interpreted by authors and researchers in different ways.

In the present paper a classification of these requirements is given. By taking into consideration the investigations, the suggested framework includes all introduced terms and concepts.

Moreover the relationship between each one of these concepts with inherent requirements of system discussed in previous section and listed in table (1), is mentioned.

1. Qualification

Only voters can vote who are qualified or have the right of voting (the ones who are a part of voters' group). Qualification is in relation with concept of R2.

2. Democracy

Only the qualified voters can vote and for only one time. Clearly this concept covers qualification feature as well. In some systems qualification is used to refer to the second section of democracy with different titles (a vote for each voter). Some examples are as following: double vote [7], not using the vote again [8,9], preventing of voting again [10]. The word democracy for instance is used in [11] and in [12] it is discussed with title of qualification. Requirement of democracy is in relation with inherent requirements of R2 and R3.

3. Correctness

This concept means:

- The outcome includes all given votes.
- The outcome depends on nothing but given votes.
- The outcome depends on the given votes as they are given.

Correctness discussed here is used in [7,11]. In [8] the word 'perfection' is used in a similar meaning with the only difference that it does not prevent dependence of outcome on matters other than given votes. In [13] perfection only covers first section and accuracy the second section of this requirement. Concept of correctness has a close relation with R4.

4. Capability of Public Verification

Consider the collection that shows given votes; the reported outcome can be verified by any one. Capability of public verification is stated in some papers such as [14,15,16,17]. In other works such as [4,8,10,18] the need to have correctness or verification capability or public acceptance capability are mentioned but any of these terms are clear enough. The term public verifiability is a more precise word and is related with R6.

5. Capability of Individual Verification

A voter must be able to check if his/her vote is counted in the way he/she voted. This issue can be found in articles such as [14,17]. In [19] this is introduced as atomic verification capability. Here similar to the public verification capability, using individual verification capability is a better substitution for this topic which is in relation with R5.

6. Privacy or Confidentiality of Vote

The definition is that the election system not to reveal vote of a voter. There are other alternative definitions; for example: “all votes must be undercover” [8,9,11] or “the relationship between vote and voter must be private” [10] or “ not making any difference between votes” [12].

There is a realty that in literature there is no agreement on definition of vote confidentiality and this shows that enough research is not done on this field until now. This requirement is in relation with R1.

7. Being without Receipt

This is when the voter cannot prove how he has voted. This concept was first introduced by [4] which was taken from concept of ‘vote buy’ and had many applications. In [20] a receipt is as a part of knowledge which is obtained only by the voter and indicates identity of voter as unique and can prove how he/she has voted. Being without receipt is in relation with R1 requirement.

8. Absence of Persuasion

This means that there should not be possibility of persuading the voter. This concept was first introduced in [5] and was discussed completely in an irregular way. In fact it was for the following sentences that this concept was introduced:

- Randomization: the voter is persuaded to vote to a random candidate
- Stimulation: the voter is persuaded to offer his/her qualification to the attacker so that the attacker vote instead of him
- Forced absence: the attacker forces voter not to vote.

Other works have introduced other concepts in this field. For example preventing persuasion of voter to vote in a special way [13,17,19]. This specification is in relation with R1.

It should be mentioned that privacy of vote, being without receipt and lack of persuasion are in relation with R1 requirement. Each one of these specifications are diverse aspects of privacy. There is not still any general agreement on these concepts.

Emergence of these kinds of concepts is due to starting a new path in researches of voting systems with capability of general inspection. These kinds of systems focus on creating ability of inspecting for the voter in every stage of voting process. This means that all activities from time of casting the vote in ballot box to the investigation of counting outcome must be checkable. In fact this concept is the same security chain performed by supervisors in paper systems.

According to what is said we perceive privacy as a collection of 6 and 7 and 8 requirements. The reason is that they are all in relation with inherent requirement of R1 and these requirements cover the concept of privacy in a general way.

3. METHODS OF PROVIDING PRIVACY

Here the how and why of choosing investigated protocols is discussed and following that findings of these investigations are presented in form of tables.

3-1 Attention to Development and Choosing Protocols

From the standpoint of related literature there is a wide range of definitions for being without receipt but the main point of it is in [4]. We know the following two plans which are of prime importance: plan [8] and plan [12]. The importance of studying these two plans is that plan [8] is designed to be used in a completely real situation. This plan is considered as implementation basis in operational voting system. In plan [12] it is tried to consider efficiency criterion in a general way. For this reason a wide range of articles attempting to present theoretical plans with purpose of accessing lack of persuasion, are inspired by this plan.

After the mentioned two plans we focused on plans without receipt. First the major work in this field presented by [4] is investigated and this procedure is continued with an alternative suggestion proposed by [6] which is proposed about the same time and covers the same subject and following that the better and more effective plans are studied.

After discussing specification of being without receipt we have investigated the new concept of privacy called absence of persuasion. Although this field is not stated clearly and completely until now, but is investigated because of its importance and influence.

3-2 Results of Studying Protocols

Results of investigations are given in the following tables. In tables the authenticity of proposed claims in mentioned protocols are investigated and encryption methods used in them are given.

Table 2. Investigated Protocols

Channels		Verification		Privacy			Protocol
$V \rightarrow A$	$A \rightarrow V$	individual	public	A. A	B R	H. R	
A	-	+	+	-	-	+	[8]
-	-	+	+	-	-	+	[12]
A	U	+	-	-	+	+	[4]
A	U	+	+	+	+	+	[21]
A	U	+	+	-	+	+	[10]
A,UA	U	+	+	-	+	+	[15]
-	U	+	+	-	+	+	[22]
P	P	+	+	-	+	+	[9]
H	H	+	+	-	+	+	[19]
H	H	+	+	-	-	+	[23]
-	-	+	+	-	-	+	[24]
H	H	+	+	-	+	+	[13]
H	H	+	+	-	+	+	[16]
U	U	+	+	-	+	+	[10]
A	U	+	+	+	+	+	[5]

Table 3. Methods of Providing Privacy

DVP	ZKP	Mystery Share	Hash networks	Homomorphic encryption	Blind Signature	Protocol
-	-	-	-	-	+	[8]
-	+	+	-	+	-	[12]
+	-	-	-	+	-	[4]

+	+	+	-	-	-	[21]
+	+	-	+	-	-	[10]
-	+	-	+	-	+	[15]
+	+	+	+	+	-	[22]
-	+	+	-	+	-	[9]
+	+	+	-	+	-	[19]
-	+	+	-	+	-	[23]
-	+	+	-	-	-	[24]
+	+	+	-	+	-	[13]
+	-	+	+	-	-	[16]
+	+	+	+	-	-	[10]
+	+	+	+	+	-	[5]

In table 2 the claim accompanied with its result of investigation in various plans considering the features of privacy , inspection capability and channels used in them which is the most important issue in determining implementation complicacy are given. In table 2, A is anonymous channel, U is untappable channel, P is private channel and H is the existence of a separate hardware for the voter in which the relation of voter with source or vice versa is shown separately. Moreover the encryption method types used in them are briefly given in table (3). In table 3 mechanisms such as double password is not discussed because these mechanisms are not used with purpose of supplying privacy.

4- CONCLUSION

In the present paper we introduced inherent requirements arisen from definition of a basic electronic voting system and compared and contrasted them with what is given other articles and as a result we presented a comprehensive framework and a more precise and formal definition of privacy in electronic voting is given. In a way that privacy of vote, being without receipt and absence of persuasion were basic parts of this requirement.

Generally two methods of blind signature encryption and homomorphic encryption are used to provide privacy. Other combinational methods are not given in this classification due to their failure in succeeding and development. As can be observed both of these methods were able to reach their goals in some ways.

In this paper we found out that taking into consideration the speed and simplicity of computations with homomorphic encryption algorithm, this method is used more; the reason is that computing the final result is usually done with only one stage of encryption while in blind signature plans the encryption stages are equal with the numbers of votes. But considering the stable structure of vote in these kinds of plans, using special channels leads to higher implementation complicacy. On the other hand for plans using blind signature the utilized blinding factor can be considered as a receipt for voter which can be presented to election personnel. Although there is such an impediment but advantages such as decreasing the use of special relational facilities has simplified implementation in them.

On the other hand plans based on blind signature by utilizing similar entities and on the basis of suggested plan in [8] are always faced with problems such as collusion of entities, addition of vote to the final outcome, changing content of vote or deleting if from final enumeration. In fact these kinds of threats inherently and hierarchically exist in all of them and in order to eliminate these problems there is a need to add computations such as adding number of entities or adding rate of transactions.

Taking into account the above statements although complicacy of implementation in blind signature plans is less but homomorphic encryption plans are prior to them due to their operational speed and reduction of transactions' rate. Besides that by giving attention to the process of development and systems' suggestion, homomorphic encryption plans, although more complicated in implementation, are more suitable for designing electronic voting protocols and privacy provision due to their higher efficiency.

5- REFERENCES

[1] http://www.electiondataservices.com, 2009.

[2] http://www.nsd.uib.no/european_election_database/country/estonia/, 2011.

[3] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 24(2):84–88, 1981.

[4] J. Cohen Benaloh and D. Tuinstra. Receipt-free secret-ballot elections (extended abstract). In Proc. 26th ACM Symposium on Theory of Computing,pages 544–553. ACM, 1994.

[5] A. Juels, D. Catalano, and M. Jakobsson. Coercion-resistant electronic elections. In Proc. 2005 ACM Workshop on Privacy in the Electronic Society, pages 61–70. ACM, 2005.

[6] D. Chaum. Secret-ballot receipts: True voter-verifiable elections. IEEE Security & Privacy, 2(1):38–47, 2004.

[7] G.Dini. Electronic voting in a large-scale distributed system. Networks, 38(1):22–32, 2001.

[8] A. Fujioka, T. Okamoto, and K. Ohta. A practical secret voting scheme for large scale elections. In Advances in Cryptology – AUSCRYPT ’92, LNCS 718, pages 244–251. Springer, 1992.

[9] B. Lee and K. Kim. Receipt-free electronic voting through collaboration of voter and honest verifier. In Proc. 2000 Joint workshop on Information Security and Cryptology, pages 101–108. Institute of Electronics, Information and Communication Engineers Japan, 2000.

[10] R. Aditya, B. Lee, C. Boyd, and E. Dawson. An efficient mixnet-based voting scheme providing receipt-freeness. In Proc. 1st Conference on Trust and Privacy in Digital Business, LNCS 3184, pages 152–161. Springer, 2004.

[11] J. Karro and J. Wang. Towards a practical, secure, and very large scale online election. In Proc. 15th Annual Computer Security Applications Conference, pages 161–169. IEEE Computer Society, 1999.

[12] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. In Advances in Cryptology EUROCRYPT’97, LNCS 1233, pages 103–118. Springer, 1997.

[13] B. Lee and K. Kim. Receipt-free electronic voting scheme with a tamperresistant randomizer. In Proc. 2002 Information and Communications Security Conference, LNCS 2587, pages 389–406. Springer, 2002.

[14] K. Sako and J. Kilian. Receipt-free mix-type voting scheme - a practical solution to the implementation of a voting booth. In Advances in Cryptology – EUROCRYPT’95, LNCS 921, pages 393–403. Springer, 1995.

[15] R. Cramer, M. K. Franklin, B. Schoenmakers, and M. Yung. Multiautority secret-ballot elections with linear work. In Advances in Cryptology – EUROCRYPT’96, LNCS 1070, pages 72–83. Springer, 1996.

[16] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang, and S. Yoo. Providing receipt-freeness in mixnet-based voting protocols. In Proc. 5th Conference on Information and communications Security, LNCS 2836, pages 245–258. Springer, 2003.

[17] M. R. Clarkson, S. Chong, and A. C. Myers. Civitas: Toward a secure voting system. In Proc. 29th Symposium on Security and Privacy, pages 354–368. IEEE Computer Society, 2008.

[18] T. Okamoto. Receipt-free electronic voting schemes for large scale elections. In Proc. 1997 Security Protocols Workshop, LNCS 1361, pages 25–35. Springer, 1997.

[19] E. Magkos, M. Burmester, and V. Chrissikopoulos. Receipt-freeness in large-scale elections without untappable channels. In IFIP Conference on E-Commerce/E-business/E-Government (I3E), pages 683–694. Kluwer, 2001.

[20] H.L.Jonker and E.P.de Vink. Formalising Receipt-Freeness, In Proc. 9th Information Security Conference, LNCS 4176, pages 476–488. Springer, 2006.

[21] V. Niemi and A. Renvall. How to prevent buying of votes in computer elections. In Advances in Cryptologo – ASIACRYPT'94, LNCS 917, pages 164–170. Springer, 1994.

[22] M. Hirt and K. Sako. Efficient receipt-free voting based on homomorphic encryption. In Advances in Cryptology – EUROCRYPT 2000, LNCS 1807, pages 539–556. Springer , 2000.

[23] O. Baudron, P. Fouque, D. Pointcheval, J. Stern, and G. Poupard. Practical multi-candidate election system. In Proc. 20th ACM Symposium on Principles of Distributed Computing, pages 274–283. ACM, 2001.

[24] A. Kiayias and M. Yung. Self-tallying elections and perfect ballot secrecy. In Proc. 5th Workshop on Practice and Theory in Public Key Cryptosystems, LNCS 2274, pages 141–158. Springer, 2002.

How to cite this article:
Pourmonfared Azimi M and Doostdari M. A. Studying privacy in electronic voting protocols and comparing its methods of provision. J. Fundam. Appl. Sci., 2016, *8(3S), 179-192.*